## AMENDMENTS TO THE SPECIFICATION

*Please amend the paragraph [0047] beginning on page 18, as follows:*

[0047] TMP3 = Rot2(TMP2) + TMP2 + 1

The instruction code set S127 includes a plurality of instruction codes that indicates to call the rotational module B144 with the variable ~~TMP2~~ TMP3, and to store the result of the operation in a variable TMP4.

TMP4 = Rot4(TMP3) XOR TMP3

The instruction code set S128 includes a plurality of instruction codes that indicates to perform an XOR operation on the variable TMP4 and the data M1, and to store the result in a variable TMP5.

5/9
A.B.

*Please amend the paragraph [0050] beginning on page ~~19~~ 20, as follows:*

[0050] TMP9 = TMP8 + K3

The instruction code set S133 includes a plurality of instruction codes that indicates to call the rotation module A143 with the variable TMP9, and to store the result of the operation in a variable TMP10.

TMP10 = Rot2(TMP9) + TMP9 + 1

The instruction code set S134 includes a plurality of instruction codes that indicates to call the rotation module ~~A143~~ D146 with the variable TMP7 and the variable TMP10, and to store the result of the operation in a variable TMP11.

*Please amend the paragraph [0052] beginning on page 20, as follows:*

[0052] TMP13 = TMP12 + K4

The instruction code set 137 includes a plurality of instruction codes that indicates to call the rotation module A143 with the variable ~~TMP14~~ TMP13, and to store the result of the operation in a variable TMP14.

TMP14 = Rot2(TMP13) + TMP13 + 1

The instruction code set S138 includes a plurality of instruction codes that indicates to perform an XOR operation on the variable TMP14 and the variable TMP4, and to store the result of the operation in a variable TMP15.

10591846

*Please amend the paragraph [0074] beginning on page 28, as follows:*

[0074] The instruction code set S223 includes an instruction code which defines data M1 and an instruction code which defines data M2. The data M1 are the 32 most significant bits of the received ciphertext M, and the data M2 are the 32 least significant bits of the received ciphertext M.

The instruction code set S224 includes a plurality of instruction codes that indicates to take the XOR operation ~~sum~~ of the data M1 and the data M2, and to store the result of this operation in a variable TMP1.

5/9
A.B.

*Please amend the paragraph [0076] beginning on page ~~28~~ 27, as follows:*

[0076] The instruction code set S226 includes a plurality of instruction codes that indicates to call the rotational module A244 with the variable TMP2, and to store the result of the operation in a variable TMP3.

TMP3 = Rot2(TMP2) + TMP2 + 1

The instruction code set S227 includes a plurality of instruction codes that indicates to call the rotational module B245 with the variable ~~TMP2~~ TMP3, and to store the result of the operation in a variable TMP4.

*Please amend the paragraph [0082] beginning on page 30, as follows:*

[0082] The instruction code set S237 includes a plurality of instruction codes that indicates to call the rotation module A244 with the variable ~~TMP14~~ TMP13, and to store the result of the operation in a variable TMP14.

TMP14 = Rot2(TMP13) + TMP13 + 1

The instruction code set S238 includes a plurality of instruction codes that indicates to perform an XOR operation on the variable TMP14 and the variable TMP4, and to store the result of the operation in a variable TMP15.